#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.3	**Incident Response (IR)[1]**					
1.	Has the Tribe or TGRA developed, documented, and disseminated an incident response policy and procedures to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI?	____	____	____	IR-1, a	
2.	Based on inquiry and record examination, does the Tribe or TGRA have an agency-level incident response policy that: • Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	IR-1, a.1.(a)	
	• Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	IR-1, a.1.(b)	
3.	Does the Tribe or TGRA have procedures to facilitate the implementation of the incident response policy and the associated incident response controls?	____	____	____	IR-1, a.2	
4.	Has the Tribe or TGRA designated an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures?	____	____	____	IR-1, b	
5.	Based on inquiry and record examination, has the Tribe or TGRA reviewed and updated the current incident response: • Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) or Criminal Justice History Record Information (CHRI) or systems used to process, store, or transmit CJI / CHRI?	____	____	____	IR-1, c.1	
	• Procedures annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI?	____	____	____	IR-1, c.2	

[1] These requirements are sanctionable for audit beginning October 1, 2024.

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
6.	Based on inquiry and record examination, does the Tribe or TGRA provide incident response training to system users consistent with assigned roles and responsibilities:					
	• Prior to assuming an incident response role or responsibility or acquiring system access?	____	____	____	IR-2, a.1	
	• When required by system changes?	____	____	____	IR-2, a.2	
	• Annually thereafter?	____	____	____	IR-2, a.3	
7.	Based on inquiry and record examination, does the Tribe or TGRA review and update incident response training content annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI?	____	____	____	IR-2, b	
8.	Based on inquiry and record examination, does the Tribe or TGRA provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach?	____	____	____	IR-2, (3)	
9.	Based on inquiry and record examination, does the Tribe or TGRA test the effectiveness of the incident response capability for the system annually using the following tests: tabletop or walk-through exercises; simulations; or other agency-appropriate tests?	____	____	____	IR-3	
10.	Based on inquiry and record examination, does the Tribe or TGRA coordinate incident response testing with organizational elements responsible for related plans?	____	____	____	IR-3, (2)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
11.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery?	____	____	____	IR-4, a	
	• Coordinate incident handling activities with contingency planning activities?	____	____	____	IR-4, b	
	• Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly?	____	____	____	IR-4, c	
	• Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization?	____	____	____	IR-4, d	
12.	Based on inquiry and record examination, does the Tribe or TGRA support the incident handling process using automated mechanisms (e.g., online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis?)	____	____	____	IR-4, (1)	
13.	Based on inquiry and record examination, does the Tribe or TGRA track and document incidents?	____	____	____	IR-5	
14.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Require personnel to report suspected incidents to the organizational incident response capability immediately but not to exceed one (1) hour after discovery?	____	____	____	IR-6, a	
	• Report incident information to organizational personnel with incident handling responsibilities, and if confirmed, notify the NIGC Information Security Officer (ISO) and FBI CJIS Division ISO?	____	____	____	IR-6, b	
15.	Based on inquiry and record examination, does the Tribe or TGRA report incidents using automated mechanisms?	____	____	____	IR-6, (1)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
16.	Based on inquiry and record examination, does the Tribe or TGRA provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident?	____	____	____	IR-6, (3)	
17.	Based on inquiry and record examination, does the Tribe or TGRA provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents?	____	____	____	IR-7	
18.	Based on inquiry and record examination, does the Tribe or TGRA increase the availability of incident response information and support using automated mechanisms that provide a push or pull capability for users to obtain incident response assistance? ***For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.***	____	____	____	IR-7, (1)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
19.	Based on inquiry and record examination, does the Tribe or TGRA develop an incident response plan that:					
	• Provides the organization with a roadmap for implementing its incident response capability?	____	____	____	IR-8, a.1	
	• Describes the structure and organization of the incident response capability?	____	____	____	IR-8, a.2	
	• Provides a high-level approach for how the incident response capability fits into the overall organization?	____	____	____	IR-8, a.3	
	• Meets the unique requirements of the organization, which relate to mission, size, structure, and functions?	____	____	____	IR-8, a.4	
	• Defines reportable incidents?	____	____	____	IR-8, a.5	
	• Provides metrics for measuring the incident response capability within the organization?	____	____	____	IR-8, a.6	
	• Defines the resources and management support needed to effectively maintain and mature an incident response capability?	____	____	____	IR-8, a.7	
	• Addresses the sharing of incident information?	____	____	____	IR-8, a.8	
	• Is reviewed and approved by the organization's/agency's executive leadership annually?	____	____	____	IR-8, a.9	
	• Explicitly designates responsibility for incident response to organizational personnel with incident reporting responsibilities?	____	____	____	IR-8, a.10	
20.	Based on inquiry and record examination, does the Tribe or TGRA distribute copies of the incident response plan to organizational personnel with incident handling responsibilities?	____	____	____	IR-8, b	
21.	Based on inquiry and record examination, does the Tribe or TGRA update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing?	____	____	____	IR-8, c	
22.	Based on inquiry and record examination, does the Tribe or TGRA communicate incident response plan changes to organizational personnel with incident handling responsibilities?	____	____	____	IR-8, d	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
23.	Based on inquiry and record examination, does the Tribe or TGRA protect the incident response plan from unauthorized disclosure and modification?	____	____	____	IR-8, e	
24.	Based on inquiry and record examination, does the Tribe or TGRA include the following in the Incident Response Plan for breaches involving personally identifiable information:					
	• A process to determine if notice to individuals or other organizations, including oversight organizations, is needed?	____	____	____	IR-8, (1) a	
	• An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms?	____	____	____	IR-8, (1) b	
	• Identification of applicable privacy requirements?	____	____	____	IR-8, (1) c	